



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,718	03/04/2002	Martin Hurich	10191/2275	4797
26646 7590 09/14/2009 KENYON & KENYON LLP ONE BROADWAY NEW YORK, NY 10004				
EXAMINER				
CERVETTI, DAVID GARCIA				
ART UNIT		PAPER NUMBER		
2436				
MAIL DATE		DELIVERY MODE		
09/14/2009		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/090,718

**Applicant(s)**

HURICH, MARTIN

**Examiner**

David García Cervetti

**Art Unit**

2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 18 May 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-12 and 15-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 and 15-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 March 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/808)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. Applicant's arguments and appeal filed 5/18/09 have been fully considered.
2. Claims 1-12 and 15-19 are pending and have been examined. Claims 13 and 14 have been cancelled.
3. **In view of the appeal brief filed on 5/18/09, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.**

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

**/Nasser G Moazzami/**

**Supervisory Patent Examiner, Art Unit 2436**

***Claim Rejections - 35 USC § 103***

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

**Claims 1-12 and 15-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest (US 5,724,428).**

**Regarding claims 1, 7, 11, and 15-17, Rivest teaches**

- a method of data encryption in programming of a control unit comprising:
- encrypting a complete stream of data to be transmitted in a programming unit using a first key, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (fig.1A-1C, col.5-6, Encryption);
- transmitting the data that had been encrypted to the control unit via a data line (fig.2, channel); and
- decrypting the data that had been encrypted in the programming unit using a second key provided in the control unit (fig.1A-1C, col.5-7, Decryption);
- wherein: successive bytes during encryption are provided with an index  $i$ , where  $i = 0, 1, 2, \dots$ , an encrypted byte  $n^*$  is formed from an unencrypted byte  $n$  according to the following, a starting value  $n_{-1}$  being used for decryption and encryption (col. 5-7):
- $n_{-1} \equiv S_0$

$$n_i^* = \left( n_i \lll \sum_{j=0}^i n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^i n_{j-1}^*\right)} \quad (\text{col. 5-7})$$

- an unencrypted byte n is formed from an encrypted byte n\* according to the following:

$$n_i = \left( n_i^* \oplus S_{h\left(\sum_{j=0}^i n_{j-1}^*\right)} \right) \ggg \sum_{j=0}^i n_{j-1}^* \quad (\text{col. 5-7})$$

Rivest does not expressly disclose the exact "equations", however teaches similar equations that accomplish the same result (col.5-7, the "for" loop accomplishes the same as the summation, and is an implementation of a summation operation). Further, the conventional DES expect the keys at both, recipient and sender, without sending the key.

Therefore, it would have been obvious to someone of ordinary skill in the art at the time the invention was made to have each participant have the key as it is taught in DES to avoid having to send it with the message.

**Regarding claims 2 and 8**, Rivest teaches wherein the first key and the second key are identical (col. 1-7, symmetric encryption).

**Regarding claims 3 and 9**, Rivest teaches wherein the first key and the second key are not identical (col. 2, variable length key, determined by parameter).

**Regarding claim 4**, Rivest teaches wherein each one of the first key and the second key includes a table that is accessed by a hash function (col. 8, hash function).

**Regarding claim 5**, Rivest teaches wherein at least one of the first key and the second key is implemented in an electronic circuit (col.1-3, hardware).

**Regarding claim 6**, Rivest teaches wherein at least one of the first key and the second key is implemented in the form of a computer program (col.1-3, software).

**Regarding claim 10**, Rivest teaches wherein the programming unit and the control unit each includes an electronic computing unit and a memory module that are linked together by a data bus (fig.1A-2, col. 1-2, microprocessor).

**Regarding claim 12**, Rivest teaches wherein the computing unit includes an electronic computing unit in a programming unit (col. 1-2, microprocessor).

**Regarding claim 18**, Rivest teaches wherein there is no bit-wise allocation between input and output data (col.3, input/output are the same size, but per round processing on bytes produces dependency on current data and intermediate results).

**Regarding claim 19**, Rivest teaches wherein there is no bit-wise allocation between input and output data (col.3, input/output are the same size, but per round processing on bytes produces dependency on current data and intermediate results).

***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID CERVETTI whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.
6. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
7. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2436

/David García Cervetti/  
Primary Examiner, Art Unit 2436